Les défis à la protection des données médicales au début du XXIe siècle

Herveg, Jean; Poullet, Yves

Published in:
Médecine & droit, information éthique et juridique du praticien

Publication date:
2006

Document Version
le PDF de l'éditeur

LES DÉFIS À LA PROTECTION DES DONNÉES MÉDICALES AU DÉBUT DU XXI^e SIÈCLE

Coordonnateurs :
***JEAN HERVEG**, Maître de conférences à la Faculté de Droit de Namur – D.E.S. D.G.T.I.C., Centre de Recherches Informatique et Droit, Avocat au barreau de Bruxelles*
***YVES POULLET**, Directeur du Centre de Recherches Informatique et Droit, P^r à la Faculté de Droit de Namur – FUNDP Professeur à la Faculté de Droit de l'Université d'État de Liège - ULg*

Langues : Français- Anglais

Cet atelier a pour objectif de fournir aux acteurs des soins de santé un aperçu global des défis majeurs qui se posent à la protection des données médicales au début du 21^e siècle en raison de l'utilisation grandissante des nouvelles technologies de l'information et de la communication dans le secteur des soins de santé et de l'apparition subséquente et logique de nouveaux risques graves d'atteintes aux droits et libertés des citoyens.
Les orateurs ont été sélectionnés de manière à fournir une approche multidisciplinaire de ces défis. Ils proviennent d'horizons différents principalement par leurs origines nationales et géographiques différentes.

Programme
1. Deryck Beyleveld, Mark Taylor, Data Protection, Genetics and Patents for BioTechnologies *(Protection des données, Génétique et Brevets pour les Bio-Technologies).*
2. Isabelle de Lamberterie, Personal and Collective Interests in the Processing of Medical Data *(Quels intérêts individuels et collectifs peut-on tirer du traitement des données relatives à la santé ?).*
3. Janlori Goldman, Benefits and Weakness of the New Federal Health Privacy Regulation – eHealth technologies – National Health Information Network (NHIN) *(Forces et faiblesses de la nouvelle réglementation fédérale en matière de protection de la vie privée et santé – Santé en ligne et technologies – Le réseau national d'information santé).*
4. Jean Herveg, The European E-Health Area : towards a Medical Data Market? *(L'espace européen de la santé en ligne : vers un marché des données médicale ?).*
5. Bartha Knoppers, The Protection of Genetic Data *(La protection des données génétiques).*
6. Roberto Lattanzi, From Medical Secrecy to Protection of Medical Data: An Overview *(Du secret médical à la protection des données médicales).*
7. Laura Vilches Armesto, Philippe Laurent, Intellectual Property Rights on Medical Data : Chimaeras and actuality *(La propriété intellectuelle sur les données médicales : chimères et réalités).*
8. Yves Poullet, ICT and Medical Data : a Challenge for Ensuring Data Protection *(TIC et Données Médicales : un défi pour assurer la protection des données).*
9. Tony Solomonides, HealthGRID.
10. Pierre Trudel, Networking Governance in E-Health Environments and Effectiveness of Data Protection Modes *(Gouvernance réseautique des environnements de cybersanté et effectivité des modes de protection des données personnelles).*

I. DATA PROTECTION, GENETICS AND PATENTS FOR BIOTECHNOLOGY

***DERYCK BEYLEVELD**, Sheffield Institute of Biotechnological Law and Ethics (SIBLE), University of Sheffield*
***MARK J. TAYLOR**, Sheffield Institute of Biotechnological Law and Ethics (SIBLE), University of Sheffield*
Correspondance : m.j.taylor@sheffield.ac.uk

This paper has three parts.
- In Part One, we argue that while biological samples and genetic information extracted from them are not (in terms of Directive 95/46/EC) personal data in and of themselves, each is capable of being personal data in appropriate contexts, and we consider the consequences of this position for data controllers and data subjects.
- In Part Two, we argue that if this is correct, then the requirement for sources of human biological samples to give informed consent for any use of their samples (which the ECJ has maintained to be a fundamental principle of EC law but not one to be enforced via patent law) must be enforced by data protection law in the EU. Furthermore, we argue that, because Directive 95/46/EC does not clearly prohibit regarding biological samples and genetic information extracted from them as personal data, the premise that the requirement for such consent is a fundamental principle of EC law supports our thesis that biological samples and genetic formation extracted from them are to be regarded personal data.
- Finally, in Part Three, we consider the implications of our position for the capacity of Directive 95/46/EC to adequately protect third party interests given the shared nature of genetic data.

II. PERSONAL AND COLLECTIVE INTERESTS IN THE TREATMENT OF MEDICAL DATA

(Quels intérêts individuels et collectifs peut-on tirer du traitement des données relatives à la santé ?)

***ISABELLE DE LAMBERTERIE**, CNRS France*

Quand on aborde la question du traitement des données de santé, le plus souvent ce sont les risques pour la protection de la vie privée induits par ce traitement qui sont étudiés. Sans nier l'existence de ces risques et l'importance des gardes fous nécessaires pour parer à ces risques, on traitera ici de façon positive des intérêts que les individus peuvent tirer du traitement des données personnelles : intérêts individuels pour la personne concernée comme pour ces proches, mais aussi intérêts collectifs de la société toute entière.

Les données de santé sont des données précieuses pour l'individu : leur traitement ou leur regroupement facilitant l'accès des personnes habilitées peut être amélioré à travers le dossier médical. Encore faut-il que celui-ci soit constitué, traité et mis à disposition dans des conditions de nature à garantir les droits fondamentaux des intéressés : droit à la confidentialité mais aussi droit à l'information. Le droit au secret pose un problème nouveau quand il s'applique aux données génétiques : celles-ci ne concernent pas uniquement une personne mais aussi les membres de sa famille. Faut-il prendre en compte ce caractère pluripersonnel pour apprécier la question soulevée par la divulgation des données génétiques d'un individu aux autres membres de sa famille ?

Les données de santé sont précieuses aussi pour la société. Parmi les données de santé qui intéressent la société, il faut faire une place particulière aux données concernant les personnes décédées. Quels sont les droits portant sur ces données ? Peuvent-elles être communiquées ? Comme nous le verrons, ces droits dépendront de la finalité du traitement et du destinataire des données. Par ailleurs, toutes les données de santé peuvent être utiles. En effet, le pilotage du système de santé dans toutes ses composantes (maîtrise des dépenses de santé, gestion du risque, épidémiologie et veille sanitaire) requiert une connaissance de plus en plus fine pour ne pas dire personnalisée de ces données. L'actualité impose de traiter, aussi, de l'importance des données de santé dans les situations de crise dites d'urgence sanitaire. Force est de constater l'insuffisance qualitative et quantitative des données relatives à l'état de santé des populations. C'est pourquoi les politiques de santé publiques recherchent aujourd'hui à concilier l'intérêt général avec le droit à la protection de la vie privée.

III. THE DEVELOPMENT OF A NATIONAL HEALTH INFORMATION INFRASTRUCTURE IN THE UNITED STATES: IMPLICATIONS FOR HEALTH CARE QUALITY, ACCESS AND PRIVACY

***JANLORI GOLDMAN**, Research Faculty, Columbia College of [illegible] and Surgeons and Director, Health Privacy Project*
Correspondance : Tél. : (212) 342-3701 - jg2408@columbia.edu

In the United States in the last few years, a number of major initiatives at the state and federal levels are moving forward to create a national network of electronic health information. The goal of many of these efforts is to enable personal health information to be created, used and shared within both the health care setting, as well as across a number of different health care and non-health environments. Proponents of such a linked system hope that, once in place and fully operational, it will improve the quality of health care in the U.S., lower the cost of providing for and paying for care, foster research and public health activities. Some supporters are eager to use health information for marketing and fundraising purposes, such as by pharmaceutical companies and hospitals.

However, a number of consumer advocacy and civil liberties groups raise the concern that unless strong and enforceable privacy and security principles and practices are put in place at the outset, a linked health information network poses a serious threat to individuals and could result in breaches of such magnitude as to undermine the overall goals of the network. In other words, if people believe that their sensitive health data might be used in ways to make them vulnerable to discrimination on the job or in health insurance, or to stigma and unwanted exposure in their communities and families, they will be more likely to withdraw from full participation in their own health care. If people do not trust that their health data will be kept confidential, they will view these emerging networks with suspicion as opposed to embracing them – as the network proponents would hope. We are at a critical juncture in the development of policies and practices where we must decide how to achieve the greatest benefits for the individual, and our communities. Yet the legal terrain is unsettled and the voice of the consumer remains unheard and often uninvolved.

Privacy law in the United States is sectoral. In April 2003, the first comprehensive health privacy law went into effect, following many years of development, and after many contentious and bitter debates. The law is the legacy of a 1996 statute known as the Health Insurance Portability and Accountability Act (HIPAA), which mandated that the U.S. Congress pass a health privacy law within three years, or the obligation to craft such a law shifted to

the Department of Health and Human Services within the Executive Branch. Due to insurmountable disagreements among various health care industries, and consumer and civil liberties groups, a legislative consensus never emerged, and the Clinton Administration was tasked with writing the law—now known as the HIPAA privacy regulation. While the law is flawed in many respects, it does create a baseline for going forward, and at this point does allow state laws that are more stringent to remain in place. The privacy regulation does cover some of proposed health information networks, but not all - and here we have the dilemma.
The HIPAA privacy rule, in brief summary, provides for the following:
• a right to see and copy your own medical records;
• the ability of health care providers, plans and "clearinghouses" to share patient records without an individual's consent for the purposes of treatment, payment, and "health care operations";
• limits on disclosures for purposes unrelated to the above, with procedural safeguards in place for disclosures to employers, law enforcement, researchers, and marketers;
• disclosures to public health as allowed by state laws;
• civil and criminal penalties may be imposed by the federal government for violations.
The gaps and weaknesses in the law include:
• the inability of an individual to sue for violation of the law;
• employers, drug companies, and others who are not health care providers or plans are not directly covered by the law if they collect health information from an individual;
• within the health care treatment and payment setting, individuals have little to no control over how their information is used and disclosed.

The implications for the development of a national health information infrastructure are vast. The HIPAA privacy regulation does impose some legal framework, but it is not comprehensive. Thus, we must decide what rules should apply in the unregulated spaces. Also, will lack of public trust erode confidence and participation in these networks, thereby undercutting their ultimate goals?
A number of efforts are underway to address the legal, policy and practice issues that are arising around how to move forward to reap the benefits to individuals, while ensuring that privacy and security is addressed. One initiative in particular is the Markle Foundation's Connecting for Health program (CFH), established a few years ago to bring together a diverse group from health care, consumer advocates, industry and government to develop models for building networks with safeguards in place. In April 2006, the CFH project will release its consensus models, protocols, policies and practices to be used by policymakers, technical experts and consumers. Whether these materials will be used widely and accepted remains to be seen, however key features include a decentralized network of health information systems, maintained at the points of entry (doctors' offices, hospitals, managed care organizations), with a Record Locator Service acting as the pointer system to the records. No uniform or unique patient identifier is required. However, this is a self-regulatory process. More detailed information will be provided in the full presentation.
Developing strong and enforceable health information privacy rules remains a critical and pressing need in the U.S., despite the HIPAA privacy rule. Not only are systems being developed that fall outside the law, but our public health systems are being transformed in the absence of open and vigorous debate. For instance, "sydromic surveillance" systems are now in place in a number of large U.S. cities, created in the wake of the September 11, 2001 terrorist attacks, and designed to report routine encounters at emergency rooms, hospitals, schools and jobs to identify unusual spikes in illnesses. At this stage, information is being shared on a daily basis with certain public health officials, not only to identify a potential bioterrorist event, but to track epidemiological events as well, such as the first flu outbreaks. However, one can imagine such a rich body of data being attractive to others outside of public health. In this way, the development of a national network of health information is both private and pubic in scope and there should be an urgency to address the policy and design issues.
How have other countries addressed these issues? How is the policy and technical environment altered by a single payer system, or within countries that have comprehensive data protection laws?

IV. L'ESPACE EUROPÉEN DE LA SANTÉ EN LIGNE : VERS UN MARCHÉ DES DONNÉES MÉDICALES ?

***JEAN HERVEG**, Maître de conférences aux FUNDP, Faculté de Droit*
Centre de Recherches Informatique et Droit
Correspondance : jean.herveg@fundp.ac.be

Dans sa communication du 30 avril 2004 au Conseil, au Parlement européen, au Comité économique et social européen et au Comité des Régions [COM(2004)356 final], la Commission européenne détaille le projet d'un espace européen de la santé en ligne, celle-ci étant l'application des technologies de l'information et de la com-

munication au secteur des soins de santé. Elle pose que la santé en ligne vise tant des outils destinés aux autorités sanitaires et aux professionnels de la santé que des systèmes de santé personnalisés pour les patients et les citoyens. Elle donne pour exemple les réseaux d'information médicale, les dossiers médicaux électroniques, les services de télémédecine, les systèmes portables de surveillance à distance des patients, les portails de santé, ainsi que tous les autres types de dispositifs fondés sur les technologies de l'information et de la communication qui fournissent des outils d'assistance à la prévention, au diagnostic, au traitement, au monitorage de la santé et à la gestion du mode de vie.
Lorsque l'espace européen de la santé en ligne sera complètement déployé, certains produits et services de la santé en ligne auront donné naissance à des bases de données médicales constituées le cas échéant sur une échelle européenne, voire mondiale. Elles pourront concerner des millions de personnes. Grâce aux nouvelles technologies de l'information et de la communication, ces bases de données pourront être facilement exploitées à diverses fins - les premières venant à l'esprit étant l'octroi de soins de santé, la recherche scientifique et médicale, la recherche de nouveaux médicaments et dispositifs médicaux. La question se pose alors de savoir si, un jour, ces nouvelles bases de données médicales ne vont pas « naturellement » aboutir à créer un marché des données médicales. La création d'un tel marché serait de nature à induire deux questions ; d'une part, la rémunération des individus pour la collecte et le traitement de leurs données médicales et, d'autre part, la rémunération du responsable du traitement pour le traitement des données médicales ou, en d'autres termes, la vente de données médicales traitées et donc aussi la question de savoir s'il faut payer pour pouvoir avoir accès à des données médicales traitées.
Si ces deux questions ne sont pas neuves en tant que telles, elles se poseront néanmoins avec une terrible acuité au regard des développements extraordinaires des technologies de l'information et de la communication dans le secteur de la santé (le mélange de l'Internet et de la technologie GRID par exemple) et de l'évolution des mœurs sociales.
La présente contribution envisage par conséquent la question de la vente par l'individu de ses données médicales et, d'autre part, la question de la vente par le responsable du traitement des données médicales traitées et de leur achat par des tiers, sans omettre la question de la répartition du prix entre la personne concernée et sa famille, le responsable du traitement, la collectivité ou l'organisme qui a financé les soins de santé, etc.

V. THE PROTECTION OF GENETIC DATA

***Bartha Maria Knoppers**, O.C., P^r of Law*
Canada Research Chair in Law & Medicine
Senior Researcher, Centre de recherche en droit public Université de Montréal

Fifteen years after the launching of the Human Genome Project, doctrinal debate on the nature of genetic information is coming to consensus. It is to be considered as sensitive medical information or even as a category of personal data subject to privacy protection.
Unfortunately, recent international policies continue to perpetuate "genetic exceptionalism". The resulting incoherence may have untoward effects on domestic legislation to say nothing of research. It also illustrates the need for both a rethinking of notions of privacy and of the process of adoption of socio – ethical and legal frameworks in an era of rapidly changing technologies.

Introduction: The "Perils" of genetic exceptionalism

Part I: Identifiability revisited
- Doubling coding/anonymization
- Reasonable and practicable
- Reasonable person/citizen

Part II: Protection of genetic information revisited
- Genetic specific/Human Rights
- Medical data protection
- Personal data protection

Conclusion: The "Promise" of privacy

VI. FROM MEDICAL SECRECY TO PROTECTION OF MEDICAL DATA: AN OVERVIEW

***Roberto Lattanzi**, Garante per la protezione dei dati personali*
Correspondance : r.lattanzi@garanteprivacy.it

1. In modern times, medical information has long played a marginal role in the legal literature. Whilst the existence of medical professional secrecy was unquestioned in terms of ethics and practice, rather than in legal terms

– often by calling for the imposition of criminal punishments –, any exceptions to this principle were left either to the lawmaker's decision, and this usually happened in the presence of a general interest considered to be overriding (in particular with a view to safeguarding public health), or to the provision of consent by the patient.

2. A number of multifarious factors have unrelentingly undermined the apparent linearity of the picture described above, especially over the past twenty-five years, and challenged the relative intangibility applying to medical information as based on professional secrecy.
It should be acknowledged that a key role in this erosion process was played by different, though cumulative, macro-factors, which will the subject of my analysis – namely: *a)* the changes in the social and economic context within which health care is provided, which have irreversibly affected the very foundations of the professional secrecy paradigm as focused on the bilateral, trust-centered relationship between a patient and his physician; *b)* the appearance of new diseases (AIDS), which have challenged the conventional assumptions (and limitations) related to professional secrecy; *c)* medical and scientific developments, in particular in the genetics sector – where the confidentiality requirements applying to personal information would appear to go beyond the individual and relate to a (more or less wide-ranging) group of individuals; *d)* technological evolution, with particular regard to the multifarious applications of information technologies within the (expanded) framework of health care activities (here reference should be made, in particular, to telemedicine, medical smart cards, and the electronic health records made available on the Internet); *e)* the increase in the so-called secondary uses of health care information within contexts other than the merely medical one (*e.g.* medical and scientific research, planning of health care and social work activities, insurance policies, employment contracts), which has been fostered in certain cases by the multi-functional nature of personal information and the cost-effectiveness of its electronic processing.

3. The co-existence of the above factors has resulted into the need for modifying the conventional approach, whereby the protection of medical information was left exclusively to professional secrecy rules.
In particular, the laws on personal data protection introduced in Europe – as well as the ad-hoc measures taken in the US legal system, where no blanket data protection law is in force – have gone beyond the conventional patient-physician relationship and the protection afforded exclusively by professional secrecy, and thus extended the protection to the data relating to one's health. In many legal systems, similar principles have also been laid down in the domestic laws concerning – generally speaking – "patients' rights" (including the issues related to processing of health care information).
However, the laws in force concerning personal data protection would not appear to be enough to regulate the multifarious uses of health care information. At least with regard to certain issues – in particular, genetics and electronic health records – it is probably necessary to set forth new-generation laws that should not be meant simply to supplement and explain the existing ones. A prerequisite to do so is the assessment of emerging law policy requirements compared with those resulting from past developments in the different legal systems.

VII. LA PROPRIÉTÉ INTELLECTUELLE SUR LES DONNÉES MÉDICALES : CHIMÈRES ET RÉALITÉS

LAURA VILCHES ARMESTO, chercheur au CRID
Correspondance : laura.vilchesarmesto@fundp.ac.be

Les données médicales sont souvent appréhendées par les juristes du point de vue de la protection de la vie privée. Nonobstant, l'on recourt fréquemment au droit de la propriété intellectuelle s'agissant de régler le contrôle, l'usage et/ou le transfert de ces données. Même si les données médicales sont relatives à des patients et font dès lors, avant tout, l'objet de règles protégeant les données personnelles et le secret professionnel, cette information est « créée », classifiée, structurée, expliquée et, de manière plus générale, traitée par des praticiens professionnels et des administrations médicales. Etant donné ce traitement de données et la rédaction de dossiers relatifs à la santé du patient, l'on pourrait penser que ces investissements intellectuels dans les dossiers des patients méritent d'être juridiquement protégés.
Existe-t-il des droits intellectuels sur les données médicales, qui en serait le titulaire et quelles en seraient les répercussions ? Ce sont les principales questions que la contribution proposée vise à aborder. L'on développera deux cas pratiques qui constitueront le fil conducteur de l'analyse : la création et la gestion du dossier médical d'un patient et l'élaboration d'une biobanque.
Un premier aperçu global de la propriété intellectuelle sera élaboré. L'on expliquera les principes et objectifs de la propriété intellectuelle, ainsi que les différents droits existants. Ensuite, parmi ceux-ci, l'on retiendra et examinera uniquement les droits qui seraient les plus susceptibles de s'appliquer aux données médicales, à savoir le brevet, le droit d'auteur et le droit des bases de données.

Pour chacun de ces droits exclusifs, l'on commencera par une brève introduction concernant l'objet, les conditions et les formalités de protection ainsi que la titularité des droits et leur usage. Cette présentation sera suivie d'une application concrète aux cas pratiques proposés. Finalement, l'on tirera des conclusions générales par rapport aux données médicales.

Au cours de l'analyse, deux hypothèses seront gardées à l'esprit: d'une part, la relation entre le patient et le praticien, et d'autre part, la relation entre les praticiens. Le but sera de déterminer si l'existence éventuelle de droits intellectuels sur les données médicales, les dossiers et/ou les analyses pourrait empêcher le patient de contrôler et/ou d'utiliser dans une certaine mesure ses données médicales, et si ces droits pourraient jouer un rôle dans le transfert de ces données médicales à des tiers (nous visons surtout d'autres praticiens) ou influencer leur accès par ces derniers.

VIII. ICT AND MEDICAL DATA: A CHALLENGE FOR ENSURING DATA PROTECTION

***P^r YVES POULLET**, Faculty of Law, Director of the CRID*
University of Namur, Belgium
Correspondance : Yves.poullet@fundp.ac.be
http://www.crid.be

ICT transform radically the traditional legal approach of the medical data processing. Different features might be underlined. The new capabilities as regards the storage notably the use of portable medical data card, the possibilities for multiplying the operations relative to medical data (including not only texts but also sounds and images), the usages of broadband networks without limitations of frontiers definitively bring to all the healthcare actors new opportunities and facilities but also create additional threats as regards the "privacy" at the largest sense of the data subjects (not only the patients but also the Healthcare practitioners).

All these features plead in favour of a better sharing of the medical data. Furthermore, new actors are intervening, taking into account the benefit they might draw down from the information circulating: social security agencies, research laboratories or public healthcare administrations but also technical services providers ensuring the transmission or the processing of certain applications.

In the past, that privacy was protected mainly by one main principle: the "professional secrecy", which does ensure the confidentiality of the relationship between the Healthcare professional and the patient. At our opinion, Data Protection laws are offering a second layer of protection which might be considered as general framework principles either for designing the different processing and flows surrounding the increasing number of possible usages of the medical data and for defining the rights and responsibilities of the different actors. It is obvious that both fundaments (Data Protection and professional secrecy) are often complementary but might lead in certain cases to contradictory solutions.

In that context, it might be useful to define these core principles and see how they have to be implemented in the new context. When can we consider that a medical data is no more a personal data and in which cases have we to impose the anonymisation of the medical data? How to ensure the respect of the "legitimate finality" and "compatibility" principles? Which place do we afford to the consent? What does mean the proportionality principle when we do consider the achievements of public interest tasks? How to apply the distinction between data controller and data processor? Apart from different concrete cases all these questions will be raised… and if possible solved.

IX. DEVICES AND DESIRES: CYBERSPACE AND THE TREATMENT OF MEDICAL DATA

***ANTHONY SOLOMONIDES**, CEMS Faculty*
University of the West of England, Bristol, BS16 1QY, UK
Correspondance : tony.solomonides@uwe.ac.uk

Grid computing ("the grid") is a promising new technology that extends the functionality and potential of the internet. It offers users a novel computational paradigm in which rapid processing, large scale data storage and flexible collaboration are made possible by harnessing together the power of large numbers of commodity computers or other clusters of basic machines, its so-called "nodes".

The grid has found many valuable medical and healthcare applications, but its underlying principles pose a major challenge to anyone seeking to deploy a grid application outside research. For example, while the grid gains its flexibility by allowing data to be stored or processed at any of its nodes, hospital authorities and other healthcare institutions must ensure that they remain in control of their confidential patient data: regulatory compliance and technology appear to be pulling in opposite directions.
We consider several similar examples and suggest approaches that retain many of the advantages of the technology while respecting the necessary legal, ethical and security frameworks. In the spirit of this paradigm, the proposed solution uses services offered by the grid to negotiate the necessary compliance according to agreed policy.

X. GOUVERNANCE RÉSEAUTIQUE DES ENVIRONNEMENTS DE CYBERSANTÉ ET EFFECTIVITÉ DES MODES DE PROTECTION DES DONNÉES PERSONNELLES

***PIERRE TRUDEL**, Centre de recherche en droit public*
Faculté de droit, Université de Montréal
Correspondance : pierre.trudel@umontreal.ca

L'adaptation du droit de la protection des données personnelles aux caractéristiques des environnements de cybersanté passe par une relecture critique des fondements et des modes de gouvernance et d'application des lois sur la protection des données de santé. Une telle relecture exige une évaluation des contextes dans lesquels circulent les informations. Dans les environnements de cybersanté, l'information est persistante et circulante. Tenter d'en empêcher la circulation au motif qu'elle pourrait être mal utilisée est une approche de moins en moins efficace. Le défi est plutôt d'assurer un cadre de gouvernance propre à garantir la qualité de l'information.
Le droit de la protection des données personnelles – hérité des approches prévalant dans les années 70-80 - impose une protection formaliste et tatillonne de protection de la vie privée. Il nie la légitimité de la circulation de certaines informations dans les réseaux de cybersanté sans pour autant assurer une protection effective des informations vraiment relatives à la vie privée. Le risque de voir se développer un ensemble de règles inadéquates aux logiques prévalant dans les environnements de cybersanté paraît suffisamment important pour justifier des interrogations sur le cadre juridique de la protection des données de santé et les approches qui pourraient en augmenter l'efficacité. Devant les rigidités découlant de plusieurs interprétations formalistes des lois sur la protection des données personnelles, tant les administrations que les législateurs ont été amenés à recourir à des expédients affaiblissant la protection des données personnelles telles que le développement de pratiques de gestion du consentement ou des lois d'exception.
Les environnements de cybersanté sont des espace de réseaux; ils comportent des espaces de gouvernance au sein desquels s'explicitent et se diffusent les normativités et les conséquences de celles-ci. Chaque environnement de cybersanté se présente comme un univers constitué de nœuds et de relais. Sa gouvernance se manifeste selon un modèle réseautique. Pour connaître les normes qui ont vocation à y assurer les régulations, il faut identifier les nœuds au sein desquels s'élabore et s'énonce la normativité. Pour s'appliquer effectivement, les principes doivent être relayés vers de multiples relais de normativité. Ce sont ces relais qui assurent l'application effective des règles.
Pour la plupart des acteurs des environnements de cybersanté, la responsabilité, notamment celle relative à la protection des données, se présente comme un ensemble de risques à gérer. Les personnes et établissements de soins doivent s'assurer que leurs pratiques sont conformes aux exigences des dispositions des règles susceptibles d'engager leur responsabilité. Ils chercheront à maîtriser les risques découlant de leurs activités en prenant les précautions susceptibles de garantir qu'elles s'en tiennent uniquement à un rôle compatible avec les responsabilités qu'elles sont prêtes à assumer.
Pour gérer adéquatement les risques, il faut généralement anticiper les conflits et identifier, de façon adaptée, comment seront relayées les exigences issues du droit ou des normativités qui risquent de trouver application. Pour gérer les risques associés aux possibles conflits, il revient aux acteurs d'expliciter leur compréhension des normativités. Les processus de gouvernance adaptés aux environnements-réseaux sont les principaux relais des normativités encadrant les activités de cybersanté. On opère ainsi l'actualisation, l'adaptation et la particularisation des règles considérées comme relevant de ces environnements d'information.